

Information Security Best Practices

MBA Regulatory Compliance May 2007

Kathryn C. Raymer

U.S. Bank Home Mortgage



Information Security

- Why is it important?
- What can you do to protect your company?
- What steps should you take if your company has a data breach?

Some Statistics

- * In the last couple of years, over 100 million records containing sensitive personal information have been breached

- Causes of breach
 - Stolen Computers
 - Lost paper documents during transport
 - Lost computer tapes during transport
 - Carelessness in transmitting data
 - Dishonest or disgruntled insider
 - Hacking

- Company Risks
 - Reputation
 - Lawsuits / \$\$
 - Loss of current customers and potential new customers

* Information obtained from Privacy Rights Clearing House – www.privacyrights.org

Information Risk Classification

- **Public Information** has been made public through authorized company channels. Information in this category includes marketing brochures, press releases, and the Annual Report.
- **Internal Information** is made available to employees and other authorized parties, such as information on company intranets or employee directories.
- **Confidential Information** provides the lender with a competitive advantage and disclosure could result in damage to you. Information in this category includes strategic business plans, financial forecasts, merger and acquisition information, and legal documents.
- **Customer Confidential Information** is a special type of confidential information about your customers, known as Sensitive Customer Information (SCI).

What is Sensitive Customer Information (SCI)?

Any combination of data drawn from two distinct categories of customer information:

- Identifier Information (ID)
 - Social Security Number
 - Drivers License Number
 - Transactional Consumer Bank Account Number
 - Credit/Debit Card Number
 - Personal Identification Number (PIN) Account Password

- Personal Data (PD)
 - Individual Name
 - Address
 - Telephone Number
 - E-mail Address

ID + PD = SCI

Creation

- Marking/Labeling (Physical)
 - Loan File Documentation
 - Miscellaneous Documentation (Reports, Memos, etc.)

- Marking/Labeling (Electronic)
 - Electronic Repositories (Shared Folders, Systems, etc.)
 - Electronic Files (Secured E-mails)

- Reproduction and Copying
 - Distribution (Need to Know)

Storage

- Physical Storage
 - Clean Desk Policy
 - Secure Locations
 - Bonding of Cleaning Crews

- Electronic Storage
 - Encryption

Sharing/Disclosure

- Conversation
 - Personal conversations
 - Phone Conversations
- Disclosure to Employees & Contractors
 - Business Need Only
- Disclosure to Third Party Business Partners
 - Vendor Management – Contractual Provisions

Transmission

- Electronic transmission on non-corporate networks
- Electronic transmission (fax)
- Mail/Delivery (Non-Company Carriers)
- Mail/Delivery (Company Carriers)
- Removal of Information from Company premises

Retention & Destruction

- Information Retention
 - Designated Areas
- Physical Document Disposal
 - Shredding
- Electronic Data Purging & Media Destruction
 - Disposal Boxes / Shredding

Key Responsibilities for Safe Guarding Customer Information

- Reinforce the importance of safeguarding SCI.
- Create an Information / Data Security Policy.
- Employees should be familiar with company Information Security Procedures.
- Employee training should be a part of your Information Security Policy.
- Companies may want to implement secured courier service.
- Employees must maintain a clean desk. All SCI should be removed from unsecured or common areas when not in use.
- Employees should shred any documentation no longer needed.
- Employees should limit their conversation. Discuss customer information only where unauthorized individuals will not hear it.
- Employees must use their computers only as authorized. Access computer systems only as required to do your job. Never share or display passwords.
- Employees must transmit internal data securely. Use sealed envelopes when distributing physical information within the company.
- Employees should only use customer information offsite as permitted, and securely. Follow appropriate safeguarding measures when utilizing confidential customer information offsite.
- Employees should log off their computer and use confidential passwords. Log off your computer at the end of the day and lock your computer when away from your workstation.

If a Breach Occurs

- Regulatory Requirements
- Have a clear Policy in effect

Additional Information

- Information Handling Table
- State Laws - Notice of Security Breach
- Sample Customer Letter